



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Craig Steen
Office: (267) 930-4735
Fax: (267) 930-4771
Email: CSteen@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 27, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent HomeRiver Group Holdings (“HRG”), located at 12906 Tampa Oaks Boulevard, Suite 100, Temple Terrace, FL 33637, and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately one (1) Maryland resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, HRG does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 16, 2024, HRG became aware of suspicious activity related to its property management database. HRG promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. Based on available evidence, the investigation determined that between July 12, 2024, and July 16, 2024, an unauthorized actor gained access to the database and acquired certain information. Accordingly, HRG undertook a thorough and in-depth review to determine what information was involved and to whom such information relates. HRG completed this process on October 31, 2024, and then moved as quickly as possible to provide notice.

The personal information related to Maryland residents that was involved includes the following: name and Social Security number.

Notice to Maryland Resident

On or about November 27, 2024, HRG provided written notice of this event to individuals whose information was identified as involved, including approximately one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, HRG moved quickly to investigate and respond to the event, assess the security of HRG's systems, and identify potentially affected individuals. As part of its ongoing commitment to information security, HRG also implemented additional administrative and technical safeguards to ensure the privacy of, and mitigate risk to, the information in its care. Further, HRG notified federal law enforcement and is cooperating with any investigation it may conduct.

HRG is providing access to credit monitoring services for one (1) year, through Cyberscout, a TransUnion company, to individuals whose personal information was potentially affected by this event, at no cost to these individuals.

Additionally, HRG is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company, bank, or other applicable institution. HRG also is providing individuals with information on how to place a fraud alert and credit freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

HRG is providing written notice of this event to relevant state regulators, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4735.

Very truly yours,

Craig Steen of
MULLEN COUGHLIN LLC

CGS/jlt

EXHIBIT A

HomeRiver Group Holdings
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



November 27, 2024

Notice of Data Breach

Dear _____ :

HomeRiver Group Holdings (“HRG”) writes to inform you of an event that may affect the security of some of your information. Although we have received no indication of identity theft or fraud as a result of this event, this notice provides you with information about the event, our response, and resources available to you to help protect your information, should you feel it is necessary and appropriate to take additional action.

What Happened? On July 16, 2024, we were alerted to suspicious activity related to our property management database. We promptly launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. Based on available evidence, the investigation determined that between July 12, 2024, and July 16, 2024, an unauthorized actor gained access to the database and acquired certain information. Therefore, we conducted a thorough and in-depth review to determine what information was potentially involved and to whom such information relates. We recently completed this process and are now providing notice.

What Information Was Involved? The investigation determined that information related to certain individuals was potentially impacted, including your name and Social Security number.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. To ensure the safety of and mitigate any risk to your information, we implemented additional safeguards to further enhance the security of data in our care. We also moved quickly to investigate and respond to the event and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering credit monitoring and fraud assistance services through Cyberscout, a TransUnion company, for twelve (12) months, at no cost to you.

What You Can Do. As always, you should remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your bank, credit card company, or other applicable institution. Additional information and resources are included in the enclosed *General Guidance to Protect Personal Information* section of this letter. You may also enroll in the complimentary credit monitoring and fraud assistance services made available to you. Enrollment instructions are attached to this letter.

000010102G0500

P

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, you may contact our dedicated assistance line at 1-800-405-6108 between the hours of 8:00 a.m. and 8:00 p.m. Eastern Time (excluding U.S. holidays). Please have this letter ready if you call. You may also contact your property manager or write to HRG at 12906 Tampa Oaks Boulevard, Suite 100, Temple Terrace, FL 33637.

Sincerely,

HomeRiver Group Holdings

GENERAL GUIDANCE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

In response to the event, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.



To enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **495C0DB6F24C**.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. You may contact HRG via phone at 1-800-405-6108.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.